Trusted CI Incident Response Report 2019-10-02_01

Post-mortem of Embargoed Singularity Report Exposure

November 1, 2019
Approved for Public Distribution
Point of contact: Von Welch (vwelch@iu.edu)

Summary

A Trusted CI engagement report with the Singularity team at Sylabs was inadvertently published prematurely due to miscommunication within the Trusted CI team. A secondary leak was discovered in the resume of a Trusted CI team member and weaknesses were discovered in the incident response process of Trusted CI. This report describes these events and the steps Trusted CI took in responding. An analysis of those events follows along with a set of planned remediations by Trusted CI to avoid a future incident and strengthen Trusted CI's incident response processes.

Background: Engagement Reports

Typically Trusted CI produces a report at the end of each of its engagements with a member of the community. These *Engagement Reports* typically describe Trusted CI's findings and recommended actions. Such reports are minimally delivered to the engaged project. When the project so agrees, reports are publicly published at the end of an engagement after review and approval by both Trusted CI and the engaged project. An *Embargoed Engagement Report* is a report whose publication is delayed by mutual agreement, typically to give the engaged party an opportunity to rectify issues discussed in the report before those issues are made public.

Trusted CI publishes reports via a scholarly archive, either IDEALS at U. Illinois or the Indiana University Scholarworks system. Both of these archives provide a sustained repository to ensure the product is available in the future as promised in Trusted CI's Data Management Plan. They also provide a *Handle* for the report: a unique, persistent handle.net URL, which guarantees an immutable reference to the report.

It is typical for Trusted CI to reserve a Handle ahead of report publication so that a citation for the report can be provided in the report. Trusted CI includes this Handle in the "Using & Citing

this Work" section of each full report. This allows parties reading a report to easily find a correct, consistent reference. To reserve a Handle in the IDEALS system, some form of PDF must be published. Typically, the report's title page is uploaded first to generate the Handle.

Trusted CI has specific team members who act as liaisons between other Trusted CI team members and the operators of IDEALS and IU Scholarworks to publish and otherwise administer Trusted CI's documents published in these services. Trusted CI liaisons do not have the ability to update documents after publication and must interface with the service operators to update a document after publication.

Primary Incident

An Embargoed Engagement Report, describing work between Trusted CI and the Singularity development team at Sylabs.io, was prematurely published by the Trusted CI team. An engagement team member was attempting to secure a Handle prior to publication and due to miscommunication, the full report, instead of the cover page, was published to the IDEALS service. There was no malicious intent. The operator of IDEALS bears no blame and no other party was involved.

Secondary Issue: Disagreement Regarding Report

A secondary issue was that the report contents were still in a state of disagreement with the Sylabs team. The Sylabs team disagreed with the language used by the Trusted CI engagement team in called the finding of Trusted CI a "vulnerability" and this issue had not been resolved at the time of premature publication.

Secondary Issue: Inclusion of Embargoed Report Content in Resume

Another secondary issue, reported to Trusted CI by Sylabs, was that content from the embargoed report was referenced with some detail, included details in dispute, in a public resume of a Trusted CI engagement team member.

Incident Timeline

Jul 26 2019 - The engagement report was published in IDEALS.

Sep 30 2019 - A third party informed the Trusted CI engagement lead that the embargoed report was public on IDEALS.

Sep 30 2019 - The engagement lead contacted the Trusted CI IDEALS publication liaison, specifically requesting that the document be removed. It was also at this time that the Trusted CI Director was informed of the incident.

Oct 1 2019 - The Trusted CI IDEALS publication liaison confirmed that the document was removed (and replaced with just a cover-sheet).

Oct 2 2019 - The Trusted CI Director asked the Trusted CI CISO (henceforth, CISO) to investigate the incident.

Oct 2 2019 - The Trusted CI ISO team (henceforth, ISO), immediately concerned with legal policy, contacted the engagement lead and verified that the report was *not* under NDA. The CISO additionally asked and learned that a notification had *not* been sent to the engagee.

Oct 3 2019 - The ISO verified that the embargoed report was no longer cached by Google.

Oct 4 2019 - The CISO contacted both the engagement lead and the IDEALS publication liaison, requesting information leading up to the premature publication in order to understand how the error came about; this led to an internal document thoroughly examining the error.

Oct 11 2019 - The CISO drafted a notification to Sylabs informing them of the data exposure, and after reviewing its contents with the engagement lead, sent the notification.

Oct 12 2019 - Sylabs responded to the ‘exposure notification’, thanking us for the notification, but expressing (i) embarrassment caused by the exposure, (ii) unwillingness to make the report public, and (iii) a desire to further discuss publication of the report. The CISO notified Trusted CI leadership of the response.

Oct 12 2019 - The Trusted CI Director assumed control of communications with Sylab and sent an apology to the engagee, expressing a desire to meet with them.

Oct 14 2019 - Sylabs reported that a content from the embargoed report was found in a resume.

Oct 15 2019 - Offending resume was removed; the Trusted CI Director informed engagee of removal.

Oct 16 2019 - Trusted CI Director informed Trusted CI’s NSF Program Officer of the incident.

Oct 17 2019 - During the NSF Cybersecurity Summit, the Trusted CI Director informed the community verbally that Trusted CI had experienced an incident, without detail, and stated that Trusted CI would publish its findings as transparently as possible.

Oct 17 2019 - Trusted CI Director and Sylabs setup a meeting for Oct 23 2019 to discuss the status of the report's publication. That meeting and a subsequent meeting have been productive with the goal being a published revised version of the engagement report.

Incident Analysis

After the incident, the Trusted CI team as a whole participated in an after action analysis. The following Findings resulted:

1. Trusted CI lacks a documented policy for labeling documents that are restricted in their distribution and the responsibilities of all Trusted CI teams members in enforcing those restrictions.

2. Trusted CI lacks a documented policy on how and when are the outcomes from its engagements are published. This includes engagee review and dispute resolution.

The analysis of Trusted CI's response to the incident yielded the following additional Findings:

3. The Trusted CI Director and CISO were not in sync with regards to their roles during incident response. Trusted CI's own Incident Response (IR) policy was insufficient to optimally guide our response. Specifically (from Trusted CI's MISPP), the directions set forth for Trusted CI's ISO define only priorities:

> *The priorities of Trusted CI Incident Response will be:*
>
> *1. Minimize loss of confidentiality of Trusted CI sensitive and engagement-related documents.*
>
> *2. Understand the scope of any loss of confidentiality, integrity or availability.*
>
> *3. Restore Trusted CI activities to normal.*

4. Communication with the engaged project was not appropriate prioritized and should have taken place sooner.

Planned Remediations

The following remediations are planned:

1. Trusted CI shall create a policy for Data labeling: how does Trusted CI label and handle documents and other work products to control their dissemination.

2. Trusted CI shall create a policy for Engagement Disclosure: How and when are the

outcomes from engagements published? This policy includes engagee review and the resolution of disputes regarding report content. The policy will also cover “side disclosure" of results in resumes, blogs, etc. by staff involved.

3. Given that these will represent Trusted CI’s first formal policies, Trusted CI will develop procedures to ensure policies are easily locatable and existing and new staff trained in their application.

4. The Trusted CI CISO will develop a more comprehensive Incident Response plan capturing key roles and responsibilities, and communication with key parties. The CISO will regularly hold *table top exercises* among the Trusted CI team to regularly educate the team and test the plans.

5. To support the other remediations, an increase of effort in the Trusted CI information security team is needed. The CISO has requested a one-time increase to .5 FTE (from .17 FTE today) for 1H2020 to implement the remediations, with ongoing effort to be determined.

To the extent it is operationally prudent, the above will be publicly available to the Trusted CI community.